Input: M, n, $e = (e_{w-1} \cdots e_2 e_1 e_0)$

Ouput: $S = M^e \bmod n$

```
Let S = 1
FOR k = w-1 downto 0
        S = (S•S) mod n
        IF (ek is 1 ) THEN
            S = (S•M) mod n
        ENDIF
ENDFOR
RETURN S
```

FIG.1(Prior Art)

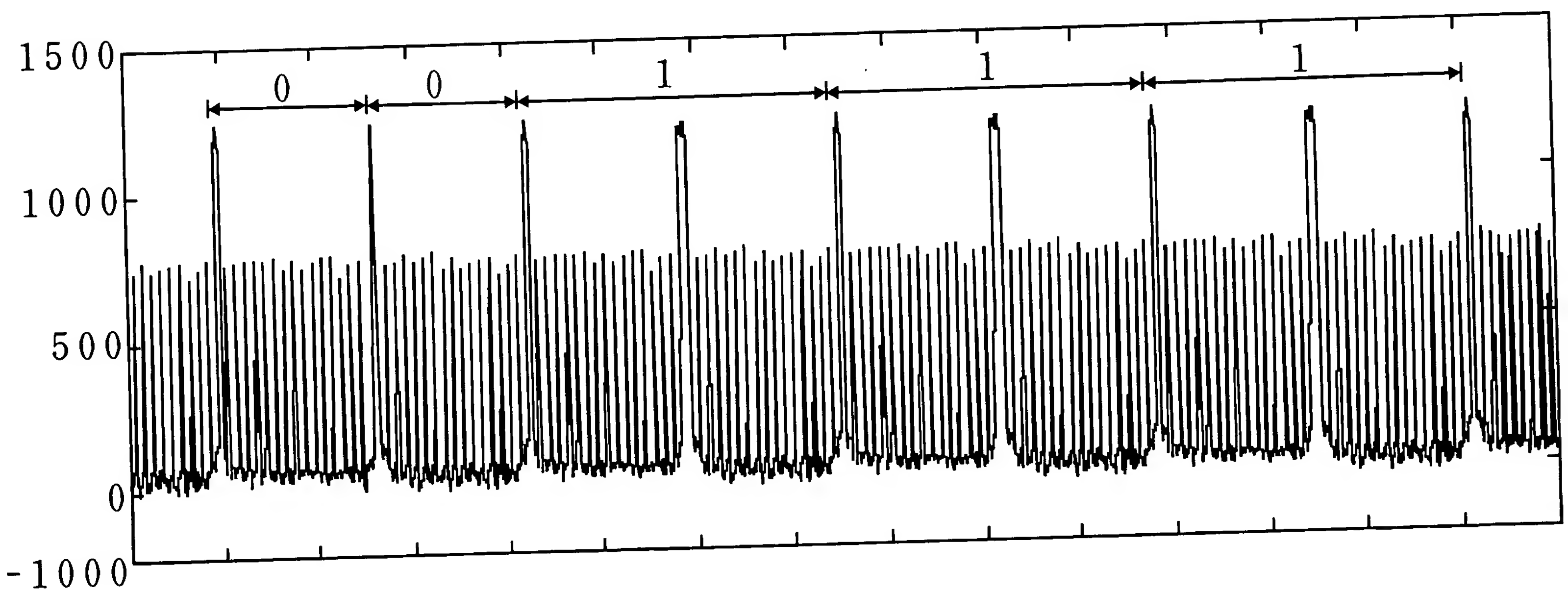

FIG.2(Prior Art)

Input: M, n, $e = (e_{w-1} \cdots e_2 e_1 e_0)$

Ouput: $S = M^e \bmod n$

Let $S_0 = 1$; $S_2 = M$

FOR $k = w-1$ downto 0

  $b = \sim e_k$

  $S_0 = (S_0 \cdot S_0) \bmod n$

  $S_b = (S_2 \cdot S_b) \bmod n$

ENDFOR

RETURN S_0

FIG.3(Prior Art)

Input: M, n, $e = (e_{w-1} \cdots e_2 e_1 e_0)$

Ouput: $S_0 = M^e \bmod n$

Algorithm : assume $e_{w-1}=1$

1. $e_{-1}=1$
2. $S_0 = 1$; $S_1 = M$
3. FOR $k = w-1$ downto 0 DO
4. $b = \sim e_k$; $c = e_{k-1}$
5. $S_0 = (S_0 \cdot S_b) \bmod n$; $S_0 = (S_0 \cdot S_c) \bmod n$

   ENDFOR
6. RETURN S_0

FIG.4

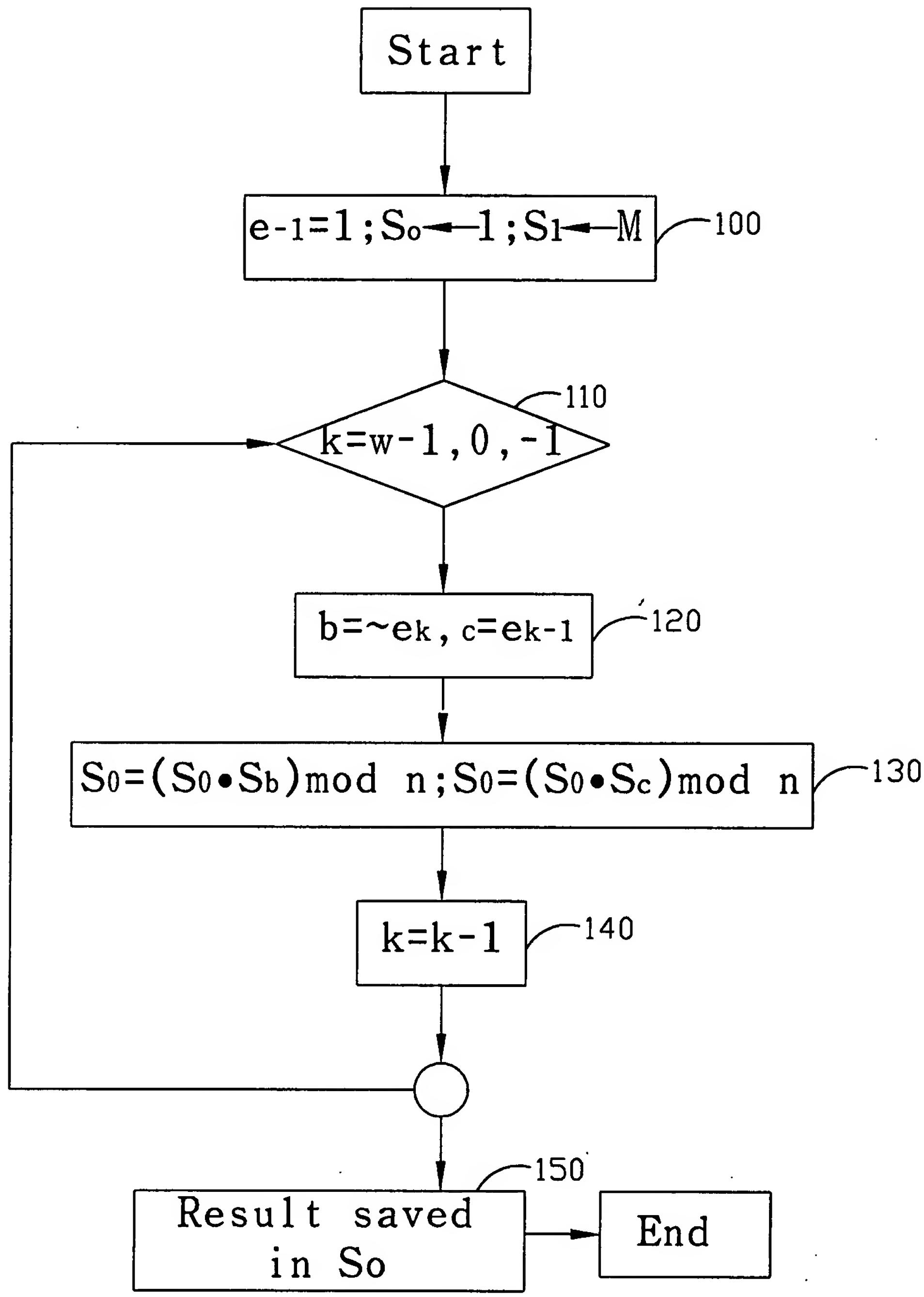
Start
$e_{-1}=1; S_0 \leftarrow 1; S_1 \leftarrow M$
100
$k=w-1,0,-1$
110
$b=\sim e_k, c=e_{k-1}$
120
$S_0=(S_0 \bullet S_b) \bmod n; S_0=(S_0 \bullet S_c) \bmod n$
130
$k=k-1$
140
150
Result saved in So
End

FIG.5

	Tracing of algorithm in Fig.1	Tracing of algorithm in Fig.6
$e_7=1$	$S=(S \bullet S) \bmod n$ $S=(S \bullet M) \bmod n$	$S_0=(S_0 \bullet S_0) \bmod n$ $S_0=(S_0 \bullet S_0) \bmod n$
$e_6=0$	$S=(S \bullet S) \bmod n$	$S_0=(S_0 \bullet S_1) \bmod n$ $S_0=(S_0 \bullet S_0) \bmod n$
$e_5=0$	$S=(S \bullet S) \bmod n$	$S_0=(S_0 \bullet S_1) \bmod n$ $S_0=(S_0 \bullet S_0) \bmod n$
$e_4=0$	$S=(S \bullet S) \bmod n$	$S_0=(S_0 \bullet S_1) \bmod n$ $S_0=(S_0 \bullet S_1) \bmod n$
$e_3=1$	$S=(S \bullet S) \bmod n$ $S=(S \bullet M) \bmod n$	$S_0=(S_0 \bullet S_0) \bmod n$ $S_0=(S_0 \bullet S_1) \bmod n$
$e_2=1$	$S=(S \bullet S) \bmod n$ $S=(S \bullet M) \bmod n$	$S_0=(S_0 \bullet S_0) \bmod n$ $S_0=(S_0 \bullet S_0) \bmod n$
$e_1=0$	$S=(S \bullet S) \bmod n$	$S_0=(S_0 \bullet S_1) \bmod n$ $S_0=(S_0 \bullet S_0) \bmod n$
$e_0=0$	$S=(S \bullet S) \bmod n$	$S_0=(S_0 \bullet S_1) \bmod n$ $S_0=(S_0 \bullet S_1) \bmod n$

FIG. 6